UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with the cellular device assigned 773-656-3562 and 312-866-0630, with listed subscriber Minister Zakar Ali that is in the custody or control of T-MOBILE US, INC., a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.	)	Case No. 22-927M(NJ)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before August 16, 2022 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 8/2/22 @ 2:40 p.m.

Nancy Joseph
Judge's signature

City and state: Milwaukee, WI Hon. Nancy Joseph, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned **773-656-3562** (referred to herein and in Attachment B as "Target Cell Phone 1") and **312-866-0630** (referred to herein and in Attachment B as "Target Cell Phone 2"), with listed subscriber Minister Zakar Ali that is in the custody or control of **T-MOBILE US, INC.** (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.
2. The Target Cell Phones.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phones for the time period **June 1, 2020 – Current Date**:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

   vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records**.**

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phones, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(B) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received) as well as per-call measurement data (also known as "real-time tool" or "RTT")].

b. Information associated with each communication to and from the Target Cell Phones for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e., antenna towers covering specific geographic areas) and sectors (i.e., faces of the towers) to which the Target Cell Phones will connect at the beginning and end of each communication, as well as per-call measurement data (also known as "real-time tool" or "RTT").

The Court has also issued an order pursuant to 18 U.S.C. § 3123, dated today, for such information associated with the Target Cell Phones.

c. Information about the location of the Target Cell Phones for a period of 30 days, during all times of day and night. "Information about the location of the Subject Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Provider, the Provider is required to disclose the Location Information to the government. In addition, the Provider must furnish the

government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider's services, including by initiating a signal to determine the location of the Target Cell Phones on the Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. Sections 1343, 1344, 1349, and 1957 (wire fraud, bank fraud, conspiracy, and engaging in unlawful monetary transactions), involving ZAKAR ALI, including, but not limited to, information pertaining to the following matters:

(a) ALI's location; and

(b) ALI's wire fraud, bank fraud, conspiracy, or unlawful monetary transaction activities.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the cellular device assigned 773-656-3562 and 312-866-0630, with listed subscriber Minister Zakar Ali that is in the custody or control of T-MOBILE US, INC., a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.

Case No. 22-927M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1343, 1344, 1349, and 1957.	Wire fraud; bank fraud; conspiracy; and money laundering.

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☒ Delayed notice of 30 days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Sarah Mazur, FBI SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 08/02/2022

Judge's signature

City and state: Milwaukee, WI

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Sarah Mazur, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A) for information about the location of the cellular telephones assigned call numbers **773-656-3562** ("Target Cell Phone 1") and **312-866-0630** ("Target Cell Phone 2"), whose service provider is T-MOBILE US, INC. ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan Way, Parsippany, NJ 07054. The Target Cell Phones are described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. In this application, the United States seeks (1) historical cell-site location information; (2) historical precision location information; (3) prospective, real-time cell-site location information; (4) prospective, real-time precision location information (i.e., E-911 Phase II data and GPS); and (5) subscriber information and other historic non-content records and information.

3. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phones.

4. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for eight years. I am currently assigned to the Milwaukee Division's Joint Terrorism Task Force, where I investigate and assist in matters involving violations of federal law related to international terrorism, domestic terrorism, and financial crimes. Prior to my time in Milwaukee, I spent approximately five years as a Special Agent in Boston investigating violent street gangs. My training and experience include the execution of arrest warrants and search warrants.

5. The facts in this affidavit come from my personal observations, my training and experience, my review of documents, and information from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that Zakar Ali ("ALI") has committed violations of 18 U.S.C. §§ 1343 (wire fraud), 1344 (bank fraud), 1349 (conspiracy), and 1957 (money laundering) (the "Subject Offenses").

JURISDICTION

7. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, this Court is "a district court of the United States that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

Background – The Small Business Administration

8. The United States Small Business Administration ("SBA") is an executive branch agency of the United States government that provides support to entrepreneurs and small

businesses. The mission of the SBA is to maintain and strengthen the nation's economy by enabling the establishment and viability of small businesses and by assisting in the economic recovery of communities after disasters.

9. As part of this effort, the SBA enables and provides for loans through banks, credit unions, and other lenders. These loans have government-backed guarantees.

The Paycheck Protection Program

10. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act was a federal law enacted in or around March 2020 and designed to provide emergency financial assistance to the millions of Americans suffering the economic effects caused by the COVID-19 pandemic.

11. One source of relief that the CARES Act provided was the authorization of up to $349 billion in forgivable loans to small businesses for payroll, mortgage interest, rent/lease, and utilities, through a program referred to as the Paycheck Protection Program ("PPP"). In April 2020, Congress authorized up to $310 billion in additional PPP funding.

12. The PPP allowed qualifying small businesses and other organizations to receive PPP loans. Businesses were required to use PPP loan proceeds on payroll costs, interest on mortgages, rent, and utilities. The PPP allowed the interest and principal on the PPP loan to be entirely forgiven if the business spent the loan proceeds on these expense items within a designated period of time and used a certain percentage of the PPP loan proceeds on payroll expenses.

13. The amount of a PPP loan that a small business was entitled to receive was determined by the number of employees employed by the business and the business's average monthly payroll costs.

14. To obtain a PPP loan, a qualifying business was required to submit a PPP loan application, which was signed by an authorized representative of the business. The PPP loan

application required the business (through its authorized representative) to acknowledge the program rules and make certain affirmative certifications in order to be eligible to obtain the PPP loan. In the PPP loan application, the small business (through its authorized representative) had to state, among other things, its: (a) average monthly payroll expenses; and (b) number of employees. These figures were used to calculate the amount of money the small business was eligible to receive under the PPP. In addition, businesses applying for a PPP loan had to provide documentation showing their payroll expenses.

15. The SBA oversaw the PPP. However, individual PPP loans were issued by private, approved lenders who received and processed PPP applications and supporting documentation, and then made loans using the lenders' own funds, which were 100% guaranteed by the SBA. Data from the application, including information about the borrower, the total amount of the loan, and the listed number of employees, was transmitted by the lender to the SBA in the course of processing the loan.

16. The CARES Act also expanded the separate Economic Injury Disaster Loan ("EIDL") Program, which provided small businesses with low-interest loans up to $2 million prior to in or about May 2020 and up to $150,000 beginning in or about May 2020, which can provide vital economic support to help overcome the temporary loss of revenue they are experiencing due to COVID-19. To qualify for an EIDL under the CARES Act, the applicant must have suffered "substantial economic injury" from COVID-19, based on a company's actual economic injury determined by the SBA, up to $2 million. EIDLs may be used for payroll and other costs as well as to cover increased costs due to supply chain interruption, to pay obligations that cannot be met due to revenue loss, and for other similar uses. The CARES Act also permitted applicants to request an advance of up to $10,000 to pay allowable working capital needs, which was expected to be

paid by the SBA within three days of submission of an EIDL application to the SBA, provided the application contains a self-certification under penalty of perjury of the applicant's eligibility for an EIDL. Unlike the PPP, the SBA directly makes loans to applicants under the EIDL Program.

THE CONSULATE OF AL MOROC LLC

17. The FBI and the Internal Revenue Service ("IRS"), Criminal Investigation Division, have been investigating ALI, Aziz Bey ("A. BEY"), Divine-Seven EL ("EL"), and Letez Bey ("L. BEY") for potential conspiracy, wire fraud, bank fraud, and money laundering offenses relating to the PPP and EIDL programs and vehicle title fraud.

18. On or about August 23, 2018, the Consulate of Al Moroc LLC ("Consulate") was incorporated in the State of Wisconsin. A. BEY was its director and registered agent. On or about January 12, 2021, A. BEY re-registered the Consulate using the name Diplomat Aziz Hassan Bey and the business address 7226 W. Marine Drive, Milwaukee, WI 53223. Based on surveillance, this address appears to be an apartment duplex in which no businesses are located. BEY does not appear to reside there but has been seen at and receives mail at this address. ALI and L. BEY also use this address on their Wisconsin identification and as a mailing address.

19. The Consulate is registered in several other states. ALI is listed as the Consulate's Treasurer in Illinois, its director in Maryland, and its president in Indiana and Florida. L. BEY is listed as the Consulate's incorporator in Indiana and Georgia and its Treasurer and registered agent in Florida. EL is listed as the Consulate's resident agent and incorporator in Maryland.

20. The Consulate is operating as a fraudulent foreign entity. The official records of the U.S. Department of State, Office of Foreign Missions, indicate that the Consulate is not registered with the Department of State and not recognized as a foreign mission in the United States.

According to those records, EL, A. BEY, L. BEY, and ALI are not registered members of a foreign mission or eligible to be diplomatic agents or consular officers.

VEHICLE TITLE SCHEME

21. An investigator with the Wisconsin Department of Transportation ("DOT") provided information to the FBI indicating that A. BEY and ALI were registering high-end vehicles with the State of Wisconsin and requesting diplomatic plates. They appeared to be engaged in "title washing," filing fraudulent paperwork with the Department of Motor Vehicles to remove a financial lienholder from a vehicle's title.

22. In or about September 2019, ALI received a $14,648 vehicle loan for a 2007 Chevrolet Trailblazer from State Farm Bank. On or about October 30, 2019, ALI registered the vehicle in Wisconsin in the Consulate's name. On or about January 22, 2020, ALI sent A. BEY an email with an attachment entitled Release of Lien, purportedly from State Farm and indicating that the lien was released as of January 25, 2020. On or about April 28, 2020, ALI attempted to pay off the loan with a $15,000 check written by EL and drawn on a closed account at PNC Bank. After the payment reversed, State Farm sent letters of delinquency to ALI and subsequently sold the loan to a collection agency.

23. According to DOT records, EL's family member gifted to the Consulate a 2018 Land Rover, which had previously been titled in Maryland. PNC Bank had a lien on the vehicle in the amount of approximately $91,000.

24. On or about July 2, 2019, A. BEY registered the 2018 Land Rover with the State of Wisconsin in the Consulate's name. A. BEY used diplomatic credentials and provided to the DOT a document dated June 21, 2019, purporting that PNC Bank released the lien on the 2018 Land Rover. According to PNC Bank, that lien release document is counterfeit.

25. On or about December 30, 2019, ALI shipped the 2018 Land Rover from Fort Lauderdale, Florida to an address in Lynwood, Illinois.

26. On or about January 17, 2020, A. BEY sold the 2018 Land Rover to Carvana LLC for $57,000. On or about April 13, 2020, EL's mother attempted to pay off the loan with a $1,000,000 check written by EL, which did not clear.

27. On or about January 27, 2020, A. BEY sent EL a cashier's check for $43,000. Based on my training and experience, I believe that the cashier's check from A. BEY represented payment for EL's participation in the title washing scheme related to the 2018 Land Rover.

28. On or about July 29, 2019, A. BEY registered with the State of Wisconsin a 2015 Lexus in the Consulate's name. The vehicle was previously titled in Maryland in the name of EL's relative with a lien from Carvana in the amount of approximately $32,000. According to records from the Maryland DOT, on or about May 22, 2019, EL's relative sold the Lexus to Union States Law Group Trust ("Trust") for $4,500. In the Maryland DOT documents, there is no record of the Carvana lien being released.

29. On or about July 28, 2019, EL signed on behalf of the Trust to transfer the vehicle's ownership to the Consulate. A search of public law enforcement databases did not yield any results for the Trust. There are no public records of this entity in Wisconsin, Maryland, or Virginia, where the Trust is purportedly located. The IRS does not have any record of an employer identification number ("EIN") being established for the Trust.

30. On or about August 19, 2019, Bridgecrest LLC (which handles financing agreements for Carvana) sent EL's relative a letter about repossessing the vehicle because the loan was in default. Prior to the issuance of the letter, Bridgecrest received a letter from the Consulate, with a $1 bill, informing it that the vehicle had been "duly claimed and registered as Foreign

Government Estate property under Trust Special Deposit." Bridgecrest was unable to repossess the vehicle and the loan was written off. On or about November 23, 2019, A. BEY sold the 2015 Lexus to Carvana for $22,604.

PPP AND EIDL PROGRAM LOAN FRAUD SCHEME

31. On or about June 22, 2020, A. BEY submitted to the SBA an online application for a loan in the amount of $108,600 under the EIDL program for the business name Aziz H Bey. On or about July 2, 2020, A. BEY signed the loan agreement electronically from an IP address located in Milwaukee. On the application, A. BEY stated that he owned a business services company with one employee that had gross revenue of $267,364. A. BEY also stated that the business was located at 7226 W. Marine Drive, Milwaukee, WI 53223, which is the business address A. BEY used when registering the Consulate with the State of Wisconsin, as discussed above.

32. Information from the Wisconsin Department of Workforce Development ("DWD") indicated that the company Aziz H Bey is not listed as an employer in Wisconsin. A search of the Wisconsin Department of Financial Institutions ("DFI") and public law enforcement databases yielded no results for the company Aziz H Bey.

33. As justification for the loan, A. BEY provided with his loan application an IRS Form 1099-MISC, used by a trade or business to report certain types of miscellaneous compensation. The Form 1099-MISC that A. BEY submitted was purportedly from the Milwaukee Area Technical College ("MATC") and included income to the business name Aziz H. Bey in the amount of $204,389 for tax year 2019. According to MATC, A. BEY had in the past been a student there but was not paid any income from MATC for 2019 or any other tax year.

34. On or about June 24, 2020, EL sent A. BEY an email with the subject line "1099misc" and containing a link to the IRS website for IRS Form 1099.

35. On or about July 7, 2020, A. BEY received funds in the amount of $108,600 under the EIDL loan program, which were deposited into A. BEY's personal checking account at TCF Bank.

36. On or about the same day he received the EIDL funds, July 7, 2020, A. BEY used cash applications to send $3,400 to ALI and $2,500 to EL.

37. On or about June 12, 2020, ALI applied online for an EIDL loan in the amount of $10,000 for the company name Zakar Ali (with trade name of Zakar Farms). The phone number he provided to SBA was **773-656-3562**. On the application, ALI stated that it was an agriculture business located in Illinois, with ten employees. ALI did not provide any supporting documentation with the loan application. A search for company Zakar Ali or Zakar Farms on the Illinois DFI and public law enforcement databases yielded no results. On or about June 15, 2020, ALI received a $10,000 advance on the loan into his personal TCF Bank account. Two days after receiving the advance, ALI withdrew $3,500 in cash. On or about September 10, 2020, the loan was declined.

38. On or about June 26, 2020, ALI applied online for a PPP loan from First Horizon Bank in the amount of $179,852 for the business Rhino Development Company LLC ("Rhino"), a company in South Carolina. On or about June 29, 2020, ALI signed the loan agreement electronically from an IP address located in Atlanta, Georgia. ALI submitted with the application Rhino's 2019 quarterly employment tax returns (Forms 941) and its Articles of Organization, listing ALI as its registered agent. According to the South Carolina Secretary of State, ALI is not listed as an agent for Rhino or any business registered in South Carolina.

39. A cooperating witness (CW-1) prepared for Rhino fraudulent Forms 941 and an ADP payroll account to get the PPP loan approved. ADP is a private company that allows other

companies to outsource their payroll and human resources functions. CW-1 had an accounting business, which allowed CW-1 to set up payroll accounts through ADP for multiple companies seeking PPP or EIDL loans. A payroll account with ADP provided legitimacy to companies such as Rhino, which in fact had no payroll. ALI and others were listed as employees in the false ADP payroll account.

40. On July 3, 2020, ALI received $179,852 in PPP loan funds wired to a First Horizon Bank account in Rhino's name, on which ALI was the only authorized signor. ALI used those funds to pay other individuals approximately $83,000 through the false ADP account, transfer approximately $22,000 to his personal account, and write a check in the amount of $71,490, which was deposited to another account in Rhino's name at SunTrust Bank.

41. On or about June 29, 2020, ALI applied online for a loan in the amount of $159,900 under the EIDL program for the business Rhino. The phone number he provided to SBA was **773-656-3562**. On or about July 14, 2020, ALI signed the loan agreement electronically from an IP address located in Atlanta, Georgia. In the application, ALI stated that the construction services business had ten employees, gross revenues of $1,299,678, and cost of goods sold of $763,290. ALI submitted with the application a copy of his Wisconsin identification listing the Consulate address in Milwaukee and Rhino's Articles of Organization, which listed ALI as the registered agent.

42. On or about July 2, and July 20, 2020, $10,000 and $149,900 of the EIDL funds, respectively, were deposited into a SunTrust bank account in the business name of Rhino. The authorized signor on that account used the funds to pay other individuals, including to an entity that paid $27,350 to ALI, which I believe represented payment for ALI's participation in the loan fraud scheme.

43. In August 2020 and January 2021, ALI applied for two EIDL loans in the business name of Drummond Hills Corporation ("Drummond"), both of which were declined. The phone number provided to SBA was **773-656-3562**. In the first online application, ALI listed Drummond as a printing/graphic design business in Miami, Florida, with two employees. ALI also listed the Consulate's address in Milwaukee as his residential address. In the second online application, ALI listed Drummond as a finance business in Lynwood, Illinois, with fifteen employees. ALI did not provide any supporting documentation.

44. In August 2020, EL sent ALI an email with an attached PDF file of the Georgia Secretary of State annual registration for Drummond. On August 10, 2020, EL (using his prior name) sent ALI an email with the subject line "SBA APP." Attached to the email was a Drummond SBA zip file containing what appeared to be screenshots of an EIDL application. On August 6, 2020, ALI sent L. BEY an email containing paperwork regarding Drummond.

45. On or about April 4, 2021, ALI applied online for a PPP loan from Capital Plus Financial in the amount of $20,832 for the company name Minister Zakar Ali. On or about April 9, 2021, ALI electronically signed the loan agreement from an IP address in Chicago. ALI used the Consulate's address in Milwaukee as the barber shop's business address.

46. Information provided from the Wisconsin DWD indicated that the company Minister Zakar Ali is not listed as an employer in the state of Wisconsin. A search for company Minister Zakar Ali on the Wisconsin DFI and public law enforcement databases yielded no results.

47. On or about June 28, 2021, ALI received $20,832 in PPP funds into his personal TCF bank account. Within days of receiving the funds, ALI withdrew approximately $5,500 in cash and used cash applications to transfer funds, including $2,000 to an individual associated with the Consulate.

48. Information received from T-Mobile on July 10, 2022, in response to legal process revealed that phone number **773-656-3562** has been subscribed to ALI since August 28, 2020, and **312-866-0630** has been subscribed to ALI since March 22, 2022. Google subscriber records also show that number **773-656-3562** is associated with ALI. And, as discussed above, ALI provided number **773-656-3562** to the SBA as his contact information on multiple occasions.

49. Obtaining information about the location of the Target Cell Phones will allow the FBI to identify targets, map patterns of travel, corroborate other evidence, and apprehend persons to be arrested.

50. Further, call detail records for the Accounts will assist investigators in documenting communications between ALI and accomplices or co-conspirators during the time period of the above-referenced activities and may reveal investigative leads or suspects.

51. In my training and experience, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

52. Based on my training and experience, I know that the Service Provider can collect cell-site data about the Target Cell Phones. I also know that wireless providers typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes. Based on my training and experience, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their normal course of business in order to use this information for various business-related purposes.

53. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training and

experience, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phones, including by initiating a signal to determine the location of the Target Cell Phones on the Service Provider's network or with such other reference points as may be reasonably available.

54. Based on my training and experience, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

55. Based on my training and experience, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes

under investigation because the information can be used to identify the Target Cell Phones' user or users and may assist in the identification of co-conspirators and/or victims.

AUTHORIZATION REQUEST

56. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

57. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control.

58. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phones on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

59. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phones would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates,

and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

60. Because the warrant will be served on the Service Provider, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phones outside of daytime hours.

ATTACHMENT A

Property to Be Searched

1. Records and information associated with the cellular device assigned **773-656-3562** (referred to herein and in Attachment B as "Target Cell Phone 1") and **312-866-0630** (referred to herein and in Attachment B as "Target Cell Phone 2"), with listed subscriber Minister Zakar Ali that is in the custody or control of **T-MOBILE US, INC.** (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan Way, Parsippany, NJ 07054.
2. The Target Cell Phones.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phones for the time period **June 1, 2020 – Current Date**:

   i. Names (including subscriber names, user names, and screen names);

   ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

   iii. Local and long distance telephone connection records;

   iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

   v. Length of service (including start date) and types of service utilized;

   vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

   vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records**.**

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phones, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(B) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received) as well as per-call measurement data (also known as "real-time tool" or "RTT")].

b. Information associated with each communication to and from the Target Cell Phones for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e., antenna towers covering specific geographic areas) and sectors (i.e., faces of the towers) to which the Target Cell Phones will connect at the beginning and end of each communication, as well as per-call measurement data (also known as "real-time tool" or "RTT").

The Court has also issued an order pursuant to 18 U.S.C. § 3123, dated today, for such information associated with the Target Cell Phones.

c. Information about the location of the Target Cell Phones for a period of 30 days, during all times of day and night. "Information about the location of the Subject Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Provider, the Provider is required to disclose the Location Information to the government. In addition, the Provider must furnish the

government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the Provider's services, including by initiating a signal to determine the location of the Target Cell Phones on the Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. Sections 1343, 1344, 1349, and 1957 (wire fraud, bank fraud, conspiracy, and engaging in unlawful monetary transactions), involving ZAKAR ALI, including, but not limited to, information pertaining to the following matters:

(a) ALI's location; and

(b) ALI's wire fraud, bank fraud, conspiracy, or unlawful monetary transaction activities.

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.